НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання лабораторної роботи

ДОСЛІДЖЕННЯ РЕАЛІЗАЦІЙ ПРОТОКОЛІВ IPSEC

Виконали студентки
групи ФІ-32мн
Зацаренко А.Ю.
Футурська О.В.

Київ — 2024

ЗВІТ

1.1 Мета лабораторної роботи

Дослідження особливостей реалізації криптографічних механізмів протоколів IPSec.

1.2 Постановка задачі

Провести дослідницьку роботу з метою аналізу особливостей реалізації криптографічних механізмів протоколів IPSec. Описати основне призначення протоколів IPSec, їх місце в мережевій моделі OSI та взаємодію зі стеком протоколів TCP/IP та ін. Дослідити архітектуру стеку протоколів IPSec. Описати призначення, особливості та відмінності криптографічних механізмів протоколів AH, ESP, ISAKMP, IKE, IKEv2, KINK та ін. Проаналізувати концепцію безпечних асоціацій (SA), її особливості та бази даних SPD і SAD (їх призначення та способи заповнення і використання). Дослідити детально особливості структури заголовків протоколів AH і ESP в тунельному та транспортному режимах з повним описанням їх полів та можливих значень. Визначити особливості обробки вхідних та вихідних IPSec-пакетів для кожного з протоколів та режимів. Дослідити нижній рівень архітектури стеку протоколів IPSec-домен інтерпретації DOI. Визначити зареєстровані алгоритми автентифікації, шифрування, геш-функцій та ін. криптографічних алгоритмів для стеку протоколів IPSec. Визначити та описати особливості основних схем застосування протоколів IPSec: хост-хост, шлюз-шлюз та хост-шлюз. А також використання протоколів IPSec для побудови VPN-тунелів.

1.3 Хід роботи

У терміні «IPsec» «IP» означає «Інтернет-протокол», а «sec» — «безпечний». Інтернет-протокол — це основний протокол маршрутизації, який використовується в Інтернеті; він визначає, куди будуть передаватися

дані за допомогою IP-адрес. IPsec є безпечним, оскільки додає до цього процесу шифрування та автентифікацію.

IPSec (Internet Protocol Security) — це набір протоколів для забезпечення безпеки даних, що передаються через мережі, включаючи Інтернет. IPSec є незамінним інструментом для забезпечення безпеки даних в сучасних мережах. Він дозволяє захистити конфіденційну інформацію від несанкціонованого доступу та забезпечити надійність мережевих з'єднань.

Протоколи IPSec безпечно передають пакети даних. Пакет даних — це певна структура, яка форматує і готує інформацію для передачі мережею. Він складається з заголовка, корисного навантаження і трейлера.

1) Заголовок — це попередній розділ, який містить інструкцію для маршрутизації пакета даних до правильного місця призначення.

2) Корисне навантаження — це термін, який описує фактичну інформацію, що міститься в пакеті даних.

3) Трейлер — це додаткові дані, що додаються до хвоста корисного навантаження, щоб вказати на кінець пакета даних.

Основні цілі IPSec:

1) Конфіденційність: Захист даних від несанкціонованого доступу за допомогою шифрування.

2) Цілісність: Перевірка того, що дані не було змінено під час передачі.

3) Автентифікація: Підтвердження справжності відправника та отримувача.

4) Захист від повторних атак: Запобігання повторній передачі перехоплених даних.

IPSec працює на рівні мережевого протоколу (3 рівень моделі OSI), тобто безпосередньо з IP-пакетами. Він додає до цих пакетів додаткову інформацію, яка забезпечує безпеку передачі, а саме: додає IP-адреси відправника (комп'ютера користувача) і одержувача (веб-сервера) до кожного пакету.

Режими роботи:

→ Транспортний режим — шифрує тільки дані у пакеті, залишаючи

заголовок IP відкритим.

→ Тунельний режим — шифрує весь IP-пакет, включаючи заголовок, і вкладає його в новий IP-пакет з новим заголовком.

Процес роботи IPSec:

1) Комп'ютер-відправник визначає, чи потребує передача даних захисту IPSec, звіряючись зі своєю політикою безпеки. Якщо так, то комп'ютер ініціює безпечну передачу даних за протоколом IPSec з комп'ютером-одержувачем.

2) Обидва комп'ютери обговорюють вимоги для встановлення безпечного з'єднання. Це включає взаємне узгодження шифрування, автентифікації та інших параметрів асоціації безпеки (SA).

3) Комп'ютер надсилає та отримує зашифровані дані, підтверджуючи, що вони надійшли з надійних джерел. Він виконує перевірки, щоб переконатися, що основний вміст є надійним.

4) Як тільки передача завершується або сеанс закінчується, комп'ютер розриває IPSec-з'єднання.

1.3.1 Концепція безпечних асоціацій (SA)

Security Association (SA) — це односторонній логічний зв'язок між двома вузлами в рамках IPsec, який визначає параметри безпеки, необхідні для захисту передачі даних. SA містить інформацію про криптографічні алгоритми, ключі, політики та параметри, які використовуються для аутентифікації, шифрування та перевірки цілісності.

Особливості SA:

1) Односторонність: SA застосовується для захисту трафіку тільки в одному напрямку (від відправника до отримувача). Для двостороннього з'єднання потрібні дві SA.

2) Ідентифікація: Кожна SA ідентифікується унікальним 32-бітовим ідентифікатором — **Security Parameters Index (SPI)**.

3) Контекст: SA працює в рамках тунельного або транспортного

режимів.

4) Типи протоколів: SA використовується як для AH (Authentication Header), так і для ESP (Encapsulating Security Payload).

Вміст SA:

– **SPI (Security Parameters Index):** Унікальний ідентифікатор SA.

– **Адреси:** IP-адреси відправника й отримувача.

– **Протокол:** Тип захисту (AH або ESP).

– **Криптографічні параметри:** Алгоритми шифрування, гешування, ключі.

– **Політики:** Час дії SA або максимальна кількість переданих пакетів.

База даних політик безпеки (Security Policy Database, SPD) містить правила та політики, що визначають, які пакети мають бути захищені, які — відхилені, а які — передані без захисту. У кожному записі SPD визначено відповідний трафік (зазвичай за IP-адресами, портами чи протоколами), а також дії, які слід виконати (захистити, пропустити або відхилити). При надходженні пакета IPsec звертається до SPD, щоб вирішити, як обробити трафік. Політики в SPD можуть бути створені вручну або автоматично налаштовані під час встановлення SA.

База даних асоціацій безпеки (Security Association Database, SAD)зберігає активні SA та їхні параметри, необхідні для забезпечення захисту трафіку. Кожен запис SAD включає SPI, криптографічні алгоритми, ключі, час дії SA, лічильники послідовності для запобігання повторним атакам, та інші метадані. Коли пакет підлягає захисту, IPsec звертається до SAD для отримання параметрів SA, пов'язаних із цим пакетом. SAD автоматично заповнюється при встановленні SA, хоча можливе й ручне налаштування.

SPD визначає політики, які визначають, чи потребує пакет захисту, а SAD забезпечує параметри безпеки для застосування цих політик. При отриманні або відправленні пакета, SPD спочатку перевіряє його відповідність правилам політики. Якщо для пакета потрібен захист, IPsec

використовує SAD, щоб знайти відповідну SA та застосувати криптографічні операції (шифрування, аутентифікація). Заповнення SPD зазвичай здійснюється адміністратором чи автоматично на основі мережевих вимог, тоді як SAD заповнюється під час узгодження SA через IKE/IKEv2.

1.3.2 IPSec у стеку TCP/IP

На відміну від стеку TCP/IP, який фокусується на доставці даних, IPSec зосереджений на забезпеченні їхньої конфіденційності, цілісності та автентичності. IPSec не є окремим стеком протоколів, він працює в межах стеку TCP/IP, забезпечуючи додатковий рівень безпеки.

Загальна схема роботи:

→ **Транспортний рівень:** Тут працюють протоколи TCP і UDP. UDP (User Datagram Protocol) — це один із основних протоколів транспортного рівня в мережевій моделі OSI та стеку TCP/IP. Його основна функція — забезпечення швидкої та ефективної передачі даних без встановлення попереднього з'єднання між відправником і отримувачем, на відміну від TCP. Дані, які потрібно передати, упаковуються в сегменти TCP або датаграми UDP.

→ **IPSec:** Між транспортним і мережевим рівнями додаються заголовки IPSec (AH або ESP або обидва). Ці заголовки містять інформацію про автентифікацію, шифрування та інші параметри безпеки. IPSec встановлює безпечне з'єднання з асиметричним шифруванням і перемикається на симетричне шифрування для прискорення передачі даних.

→ **Мережевий рівень:** Додається IP-заголовок, який містить IP-адреси відправника та одержувача.

→ **Канальний рівень:** Дані передаються по фізичному середовищу (кабель, Wi-Fi тощо).

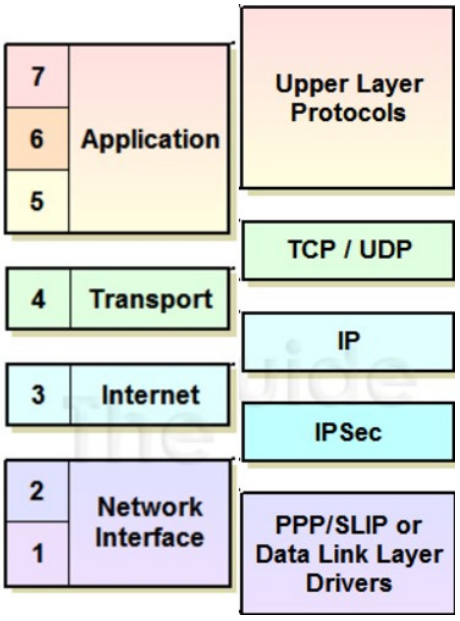

Рисунок 1.1 – Схема з і без IPSec

1.3.3 Протоколи AH і ESP

У стеку TCP/IP IPSec інтегрується в IP-рівень (Internet Layer). Він доповнює базову функціональність IP наступними протоколами:

1) **AH (Authentication Header):** Забезпечує цілісність і аутентифікацію даних, але не виконує шифрування. AH створює геш (англ. Message Authentication Code, MAC) для контрольованих даних пакета, використовуючи криптографічний алгоритм (наприклад, HMAC-SHA-1 або HMAC-SHA-256). До гешування включаються такі частини IP-пакета:

– Поля IP-заголовка, які залишаються незмінними під час передачі.

– Корисне навантаження (payload) — основна інформація або дані, які передаються в мережевому пакет.

Заголовок AH вставляється між IP-заголовком та корисним навантаженням. Він містить:

– Ідентифікатор безпеки (англ. Security Parameters Index, SPI).

– Лічильник послідовності (англ. Sequence Number) — лічильник послідовності пакетів, який запобігає повторному використанню одного й того ж пакета атакуючим.

– Геш (MAC).

2) **ESP (Encapsulating Security Payload):** Забезпечує шифрування, а також цілісність і автентифікацію. Корисне навантаження шифрується за допомогою алгоритмів, наприклад AES і весь зашифрований текст стає недоступним для перегляду. Якщо увімкнена функція автентифікації, ESP розраховує MAC, як і AH. Заголовок ESP додається перед зашифрованим корисним навантаженням і включає:

→ Ідентифікатор безпеки (англ. Security Parameters Index, SPI).

→ Лічильник послідовності (англ. Sequence Number).

Після зашифрованого корисного навантаження додається ESP Trailer (визначає розмір і вирівнювання).

ESP може працювати у двох режимах:

– **Транспортний:** Захищає тільки корисне навантаження, залишаючи оригінальний IP-заголовок. Цей режим часто використовується для наскрізного зв'язку між двома хостами або пристроями в мережі.

– **Тунельний:** Інкапсулює весь оригінальний IP-пакет (заголовок + дані), додаючи новий IP-заголовок. Цей режим зазвичай використовується для створення захищених VPN-мереж типу «сайт-сайт» або віддаленого доступу, де оригінальний IP-пакет захищається як єдине ціле під час проходження через ненадійну мережу.

Режим	**Протокол**	**Особливості обробки**
Транспортний	AH	Захищає цілісність заголовка та корисного навантаження, але не шифрує дані.
	ESP	Шифрує корисне навантаження (TCP/UDP і дані), може забезпечувати автентифікацію.
Тунельний	AH	Автентифікує весь оригінальний IP-пакет, але не забезпечує шифрування.
	ESP	Шифрує і захищає весь внутрішній IP-пакет, включаючи його заголовок і дані.

Таблиця 1.1 – Особливості обробки протоколів AH та ESP у різних режимах

1.3.4 Обмін ключами в Інтернеті (IKE)

Обмін ключами в Інтернеті (англ. Internet Key Exchange, IKE) — це протокол, який встановлює безпечне з'єднання між двома пристроями в Інтернеті. Обидва пристрої встановлюють асоціацію безпеки (SA), яка передбачає узгодження ключів шифрування та алгоритмів для передачі та отримання наступних пакетів даних.

ISAKMP (Internet Security Association and Key Management Protocol) є базовим фреймворком, який забезпечує механізми обміну ключами та управління SA. ISAKMP — це протокол, який використовується для створення, узгодження та управління SA незалежно від конкретних криптографічних алгоритмів. Він визначає формат і методи обміну інформацією, необхідною для створення захищених з'єднань, але не займається безпосередньо обміном ключами. ISAKMP є основою для таких протоколів, як IKE, які реалізують конкретні механізми обміну ключами та автентифікації. Його гнучкість забезпечує сумісність між різними системами і криптографічними методами.

IKE та **IKEv2** — це протоколи, які використовують ISAKMP для встановлення захищених з'єднань.

IKE — це протокол, який працює в рамках IPsec для встановлення захищених каналів зв'язку. Він виконує взаємну автентифікацію між сторонами, що спілкуються, узгоджує SA і полегшує обмін криптографічними ключами. IKE працює у два етапи: на першому етапі встановлюється безпечний канал, а на другому - узгоджуються додаткові SA для захищеного потоку даних. Незважаючи на свою надійність, його складність призвела до розробки покращеної версії, IKEv2.

IKEv2 — це вдосконалена версія IKE, розроблена для усунення недоліків попередньої версії. Вона спрощує процес переговорів, об'єднуючи етапи в єдину впорядковану процедуру, зменшуючи затримки та підвищуючи продуктивність. IKEv2 також забезпечує кращу обробку мережевих змін, таких як оновлення IP-адрес, що робить його ідеальним

для мобільних середовищ. Він підтримує сучасні криптографічні алгоритми та покращує обробку помилок. Ці вдосконалення роблять IKEv2 безпечнішим і швидшим, залишаючи при цьому зворотну сумісність з IKE.

KINK, Kerberized Internet Negotiation of Keys — це протокол обміну ключами, який можна використовувати з IKE для підвищення безпеки. На відміну від IKE, він усуває потребу в попередньо наданих ключах або інфраструктурі відкритих ключів (PKI), покладаючись на Центр розподілу ключів Kerberos (KDC). KINK спрощує керування ключами в системах на основі Kerberos і забезпечує безпечний динамічний обмін ключами без обчислювальних витрат IKE. Однак, він менш поширений і в першу чергу підходить для корпоративних або закритих мережевих сценаріїв використання Kerberos.

Kerberos — це протокол мережевої автентифікації, призначений для забезпечення безпечної автентифікації між користувачами та сервісами в розподіленій мережі. Він використовує модель довіреної третьої сторони, покладаючись на центральний центр розподілу ключів (KDC) . Kerberos забезпечує взаємну автентифікацію, тобто клієнт і сервер перевіряють ідентичність один одного. Він широко використовується в корпоративних середовищах.

1.3.5 Домен інтерпретації (DOI) у стеку протоколів IPsec

Домен інтерпретації (DOI) є нижнім рівнем архітектури IPsec, який визначає узгоджений набір параметрів і правил для встановлення безпечних з'єднань. DOI забезпечує стандартизацію конфігурацій SA, параметрів криптографії та використання IKE/IKEv2. Він включає ідентифікацію протоколів (AH, ESP), підтримуваних алгоритмів, політик захисту та механізмів узгодження параметрів між сторонами. DOI також визначає параметри, такі як Security Parameters Index (SPI), час життя SA і механізми обробки трафіку, забезпечуючи взаємодію між різними системами.

IPsec підтримує широкий спектр криптографічних алгоритмів для забезпечення гнучкості. Серед алгоритмів автентифікації — HMAC-SHA1, HMAC-SHA2 (SHA-256/384/512) та AES-GMAC. Для шифрування використовуються DES, 3DES, AES (з режимами шифрування CBC, GCM, CCM). Геш-функції включають MD5 (застарілий), SHA-1 і SHA-2. Алгоритми групової криптографії для узгодження ключів — MODP (групи Диффі-Геллмана) та ECP (еліптичні криві). Зареєстровані алгоритми регулярно оновлюються, щоб відповідати сучасним стандартам безпеки.

1.3.6 Основні схеми застосування IPsec

– **Хост-хост:** Забезпечує захищений зв'язок між двома кінцевими вузлами без посередників. Використовується для прямого шифрування або аутентифікації даних між комп'ютерами, наприклад, у внутрішніх корпоративних мережах.

– **Шлюз-шлюз:** Створює захищений тунель між двома мережевими шлюзами. Уся комунікація між мережами проходить через цей тунель, що є типовим для міжофісних з'єднань.

– **Хост-шлюз:** Використовується, коли хост з'єднується із захищеною мережею через шлюз. Цей підхід часто застосовується для віддаленого доступу, наприклад, співробітниками, які підключаються до корпоративної мережі.

1.3.7 Використання IPsec для побудови VPN-тунелів

VPN, або віртуальна приватна мереж — це мережеве програмне забезпечення, яке дозволяє користувачам анонімно і безпечно користуватися Інтернетом. IPSec VPN — це програмне забезпечення VPN, яке використовує протокол IPSec для створення зашифрованих тунелів в Інтернеті. Вона забезпечує наскрізне шифрування, тобто дані шифруються на комп'ютері і розшифровуються на приймаючому сервері.

Багато VPN використовують набір протоколів IPsec для встановлення

та запуску цих зашифрованих з'єднань. Однак не всі VPN використовують IPsec. Іншим протоколом для VPN є SSL / TLS , який працює на іншому рівні в моделі OSI, ніж IPsec.

Протоколи IPsec є одним із найбільш поширених рішень для створення VPN-тунелів завдяки високому рівню безпеки, який забезпечується шифруванням, автентифікацією, і перевіркою цілісності даних. У VPN на основі IPsec трафік між двома точками (наприклад, хостами чи шлюзами) інкапсулюється в захищений тунель. Це зазвичай реалізується в **тунельному режимі**, коли весь оригінальний IP-пакет шифрується і вкладається в новий IP-заголовок, що приховує внутрішні IP-адреси і захищає інформацію від перехоплення.

VPN дають змогу безпечно отримувати доступ до конфіденційних даних і обмінюватися ними через спільну мережеву інфраструктуру, таку як публічний Інтернет. Наприклад, коли співробітники працюють віддалено, а не в офісі, вони часто використовують VPN для доступу до корпоративних файлів і програм.

ВИСНОВКИ

IPSec є потужним інструментом для захисту мережевих з'єднань. Його багатошарова архітектура дозволяє забезпечити комплексну безпеку даних, а використання сучасних криптографічних алгоритмів робить його надійним для застосування в сучасних мережах. IPSec часто використовується для побудови VPN, забезпечуючи безпечну передачу даних між віддаленими вузлами.